Rules of Behavior for Use of Computer Systems

The rules listed below are for the use of Information Technology (IT) resources operated by NASA Center personnel. The purpose is to increase individual awareness and responsibility, and to ensure that all users use the Center's IT resources in an efficient, ethical, and lawful manner.

I, (please print)_____________________________________, understand that:

1. The computer system I am requesting an account for may only be used for official purposes in the conduct of my duties.

2. All software on the computer system is protected in accordance with NASA and Federal Government security and control procedures which will be adhered to. Licensed software will only be used in accordance with the license.

3. Use of these IT resources gives consent for monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for Center IT resources.

4. Electronic communications facilities (such as e-mail and Netnews) are for authorized Government use only. Center IT resources will not be used for fraudulent, harassing or obscene messages and/or materials.

5. When access is no longer required to these IT resources, I must notify appropriate responsible parties and make no further attempt to access these resources.

6. The CNE Project purchased the Annex to provide GSFC personnel with a means to connect to the Goddard network from home or while on travel. Its intent is to allow users a method of checking e-mail and doing other limited work from home or while on travel. This is a government computer resource, for use by government employees and approved contractors, and is to be used only for government related work. If it is discovered that resources are being misused, your dial-up account will be deleted and further appropriate action may be taken.

7. No IT resources will be removed from a NASA Center without a property pass from the property custodian.

8. Fixed media will be erased prior to transferring the IT resources or designating the resource for excess.

9. Tampering with another user's account, files, or processes without the other user's express permission; use of the system resources for personal purposes; or other unauthorized activities is strictly prohibited and will result in disciplinary action.

10. Logon ID's and passwords may never be transferred or shared for any reason.

11. Active logons should never be left unattended. Workstations will be paused when unattended for short periods of time (less than 30 minutes).

1A.2. Do not logon to more than one workstation/terminal unless you can keep each of them under constant surveillance.

1A.3. Passwords:

a. will be a minimum of 8 alphanumeric characters containing at least one character each from at least three of the following sets of character: uppercase letter, lowercase letters, numbers, special characters

b. will be changed in accordance with NASA Procedures and Guidelines (NPG 2810.1) for the corresponding the data, application or system information category (see Section A.6.3.4)

c. will not be a word appearing in an English or foreign dictionary

d. will be memorized and not written down

e. will not be stored in keyboard macros or .bat files
f. will not consist of personal ID data or be easily guessable
14. Challenge anyone in the computer facility who does not have an appropriate badge.
15. Rooms with workstations or terminals must be locked after normal working hours except when such workstations or terminals are located in continuously manned operational areas.
16. Access to and use of the Internet will only be for official purposes in the conduct of your duties.
17. Personally owned, provided, or downloaded software may not be installed without management approval.
18. E-mail will only be used for official purposes and will not be used to transmit the following information:

- a. U.S. Government or corporate credit card numbers
- b. Designated Sensitive Data
- c. Risk Assessments
- d. For Official Use Only information
- e. Privacy Act Data
- f. Proprietary Data
- g. Procurement Sensitive Data
- h. Source Evaluation Board (SEB) information

19. Any unauthorized penetration attempt, unauthorized system use, or virus activity will be reported to your supervisor.
20. Failure to adhere to these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.
21. Signing the front of this form indicates that you have read, understand, and will comply with these rules.
I further understand that failure to abide by these rules may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

I HAVE READ AND UNDERSTAND THE RULES OF BEHAVIOR FOR THE USE OF THE EOSDIS INFORMATION TECHNOLOGY (IT) RESOURCES AND AGREE TO ABIDE BY THEM.

I fully understand my responsibilities as a user of this system/network.

User Name: (please print)____

User Signature:____
:
Organization Code/Contractor Name:____

Date: _______________________